

IN THE CLAIMS

1-14 (Canceled).

15. (New) A certificate comprising:

an electronic tag attached on or put in the certificate and storing a first information;
wherein a second information and a digital signature are printed on the surface of the certificate; and
the digital signature is generated from the first information and the second information.

16. (New) The certificate according to claim 15;

wherein the digital signature is generated from a linkage or a hashed linkage of the first information and the second information using RSA.

17. (New) The certificate according to claim 15;

wherein the digital signature is a sum or a hashed sum of the first information and the second information using RSA.

18. (New) The certificate according to claim 15;
wherein the first information is represented by x_1 ,
the second information is represented by x_2 and the digital
signature is represented by y , secret keys are represented by
 d and n , and the digital signature is obtained by the equation
$$y = (x_1 + x_2) ^* d \bmod n$$
, where the function "+"
represents linking of x_1 and x_2 to each other.

19. (New) An apparatus for issuing a certificate
comprising:

a certificate paper-accommodating part which
accommodates certificates comprising electric tags which
stores first information;

a printing part which prints a second information
and a digital signature on the surface of the certificates;
and

wherein the digital signature is generated from the
first information and the second information.

20. (New) The apparatus according to claim 19;

wherein the digital signature is generated from a linkage or a hashed linkage of the first information and the second information using RSA.

21. (New) The apparatus according to claim 19;

wherein the digital signature is a sum or a hashed sum of the first information and the second information using RSA.

22. (New) The apparatus according to claim 19;

wherein the first information is represented by x_1 , the second information is represented by x_2 and the digital signature is represented by y , secret keys are represented by d and n , and the digital signature is obtained by the equation $y = (x_1 + x_2) ^{**d} \bmod n$, where the function "+" represents linking of x_1 and x_2 to each other.